



Karta przedmiotu

Nazwa i kod przedmiotu	Wprowadzenie do cyberbezpieczeństwa, PG_00053947						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu			2027/2028		
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć			Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	2	Język wykładowy			polski		
Semestr studiów	4	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Teleinformatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr inż. Wojciech Gumiński				
	Prowadzący zajęcia z przedmiotu		dr inż. Wojciech Gumiński				
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	0.0	15.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach	Praca własna studenta	RAZEM	
	Liczba godzin pracy studenta	30		2.0	18.0	50	
Cel przedmiotu	Celem przedmiotu jest nauczenie studenta podstaw związanych z cyberbezpieczeństwem. W ramach przedmiotu studenci poznają wybrane zagrożenia dla bezpieczeństwa. Prezentowany jest zbiór funkcji bezpieczeństwa, m. in.: poufność, integralność i dostępność wraz z mechanizmami pozwalającymi na ich realizację. W ramach zajęć praktycznych studenci nabywają umiejętności operowania materiałem kryptograficznym w podstawowych, popularnych scenariuszach użycia.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K6_K03] jest gotów do wypełniania zobowiązań społecznych, współorganizowania działalności na rzecz środowiska społecznego, inicjowania działania na rzecz interesu publicznego, myślenia i działania w sposób przedsiębiorczy	Student potrafi zaimplementować kryptograficzne zabezpieczenie informacji.	[SK1] Ocena umiejętności pracy w grupie [SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce
	[K6_U03] potrafi zaprojektować, zgodnie z zadaną specyfikacją, oraz wykonać typowe dla kierunku studiów proste urządzenie, obiekt, system lub zrealizować proces, używając odpowiednio dobranych metod, technik, narzędzi i materiałów, korzystając ze standardów i norm inżynierskich, stosując właściwe dla kierunków studiów technologie i wykorzystując doświadczenie zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską	Student potrafi praktycznie wykorzystać poznane rozwiązania bezpieczeństwa. W ramach prac projektowych integruje/ implementuje i prezentuje ich zastosowanie w określonym scenariuszu użycia.	[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania [SU1] Ocena realizacji zadania
[K6_W44] zna i rozumie w zaawansowanym stopniu architektury, zasady projektowania oraz metody wsparcia sprzętowego i programowego dla lokalnych i rozproszonych systemów informatycznych, w tym systemów obliczeniowych, baz danych, sieci komputerowych i aplikacji informacyjnych, zasady współpracy człowieka z komputerem, a także działanie i kryteria oceny metod przetwarzania, składowania i przesyłania danych, w tym algorytmów obliczeniowych, sztucznej inteligencji i eksploracji danych oraz standardy i metody administrowania systemami informatycznymi, monitorowania zachodzących w nich procesów oraz uodporniania ich na niepożądane zjawiska i działania	Student wymienia i opisuje atrybuty bezpieczeństwa. Student wymienia różnice między algorytmami kryptografii symetrycznej i asymetrycznej oraz potrafi podać przykłady ich zastosowań.	[SW1] Ocena wiedzy faktograficznej	
Treści przedmiotu	Treści przedmiotu - wykład Podstawowe pojęcia związane z bezpieczeństwem systemów IT, funkcje bezpieczeństwa: integralność, poufność, uwierzytelnianie. Rodzaje zagrożeń i ataków: poznanie treści, modyfikacja treści, podszywanie, ataki celowane i niecelowane, malware, sieci botnet. Wprowadzenie do kryptografii: k. symetryczna i asymetryczna, klucze jednorazowe, szyfry blokowe i strumieniowe, integralność danych. Kryptografia klucza publicznego i PKI. Bezpieczeństwo w zastosowaniach: zastosowania PKI, obsługa rozwiązań wykorzystujących certyfikaty. Podstawy zarządzania bezpieczeństwem: polityka bezpieczeństwa, dobre praktyki bezpieczeństwa, dobre praktyki rozwijania bezpiecznego kodu.		
Wymagania wstępne i dodatkowe	Znajomość konfiguracji i obsługi popularnych systemów operacyjnych		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	Ocena z projektu	50.0%	50.0%
	Ocena z części wykładowej	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	Materiały i prezentacje do zajęć	
	Uzupełniająca lista lektur	Schneier B.: Kryptografia dla praktyków Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych Stallings W.: Cryptography and Network Security Gollmann D.: Computer security	
	Adresy eZasobów		

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none">1. Implementacja wybranych algorytmów szyfrowania symetrycznego przy użyciu dostępnych bibliotek2. Wykorzystanie infrastruktury klucza publicznego na potrzeby wzajemnego uwierzytelniania klientserwer WWW3. Wykorzystanie infrastruktury klucza publicznego na potrzeby podpisywania i szyfrowania poczty email
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.